Penerapan Firewall sebagai Mekanisme Pengendali Akses Jaringan dengan Cisco Packet Tracer

Sayudha Hanif Saputra* [1], Raditya Duta Pratama[2], Yarsis Febriansyah Putra[3], Indrawan Ady Saputro[4]
[1234]PRODI S1 INFORMATIKA, STIMIK AMIKOM SURAKARTA
[1234]SUKOHARJO INDONESIA
Email: [1]sayudha.130527@mhs.amikomsolo.ac.id,
[2]raditya.130549@mhs.amikomsolo.ac.id, [3]yarsis.130528@mhs.amikomsolo.ac.id,
[4]indrawanadys@dosen.amikomsolo.ac.id

Abstract

This research discusses the implementation of network security using firewall and port security methods on Cisco Packet Tracer. The system is designed to simulate the access control between server and client PCs through firewall rules applied to the server. The firewall configuration is based on the IP address of each client to either allow or deny communication. This configuration ensures that only authorized IP addresses can communicate with the server, while unauthorized IPs are blocked. The simulation involves one server and three PCs connected via a switch. IP configuration and firewall rules are implemented and tested using Cisco Packet Tracer. The result shows that the firewall effectively restricts access as intended. This method is relevant for network administrators to control network traffic and improve security in small to medium-sized networks.
Keywords: *access control, Cisco Packet Tracer, firewall, IP filtering, network security*

Abstrak

Studi ini mengkaji penerapan perlindungan jaringan melalui pendekatan firewall dan pengamanan port menggunakan Cisco Packet Tracer. Sistem tersebut dirancang untuk memodelkan pengendalian akses antara server dan PC klien dengan menerapkan kebijakan firewall pada server. Pengaturan firewall dipastikan berdasarkan alamat IP setiap klien, untuk mengizinkan atau menolak interaksi. Pengaturan ini menjamin bahwa hanya alamat IP yang memiliki otorisasi yang dapat berkomunikasi dengan server, sedangkan IP yang tidak memiliki izin akan diblokir. Simulasi melibatkan satu server dan tiga PC yang terhubung melalui switch. Konfigurasi IP dan kebijakan firewall diimplementasikan serta diuji menggunakan Cisco Packet Tracer. Hasilnya menunjukkan bahwa firewall secara efektif membatasi akses sesuai harapan. Pendekatan ini penting bagi administrator jaringan dalam mengatur lalu lintas jaringan guna meningkatkan keamanan pada jaringan berskala kecil hingga menengah.

Kata Kunci: Cisco Packet Tracer, firewall, perlindungan jaringan, pengendalian akses, pemfilteran IP

1. PENDAHULUAN

Keamanan jaringan merupakan aspek penting dalam menjaga kerahasiaan, integritas, dan ketersediaan informasi. Seiring meningkatnya kebutuhan organisasi terhadap layanan berbasis jaringan, ancaman seperti malware, akses ilegal, sniffing, dan serangan DoS semakin berkembang dan kompleks. Firewall menjadi salah satu

mekanisme pengendalian akses yang umum digunakan karena mampu menyaring lalu lintas berdasarkan aturan tertentu.

Berbagai penelitian sebelumnya telah membahas implementasi firewall maupun port security pada lingkungan jaringan (*[1][2][3]*). Namun, sebagian besar penelitian tersebut berfokus pada pengujian skala besar, penggunaan perangkat nyata, atau konfigurasi tingkat lanjut seperti ASA, VPN, atau ACL kompleks. Gap penelitian yang muncul adalah kurangnya kajian yang secara spesifik membahas efektivitas firewall sederhana berbasis IP filtering pada skenario jaringan kecil (1 server – 3 client) menggunakan Cisco Packet Tracer, yang umum digunakan pada lingkungan pendidikan dan laboratorium pembelajaran dasar jaringan.

Selain itu, penelitian sebelumnya jarang mengukur efektivitas firewall secara kuantitatif pada skenario paling dasar, yaitu bagaimana firewall memblokir dan mengizinkan koneksi berdasarkan aturan sederhana. Oleh karena itu, penelitian ini mencoba mengisi kekosongan tersebut dengan mensimulasikan konfigurasi firewall berbasis IP pada topologi kecil, sekaligus memberikan data kuantitatif mengenai hasilnya.

Penelitian ini bertujuan untuk memberikan pemahaman praktis tentang implementasi firewall dasar menggunakan Cisco Packet Tracer, serta mengukur tingkat keberhasilan firewall dalam mengendalikan akses pada jaringan lokal. Dengan pendekatan ini, diharapkan pembaca dapat memahami efektivitas firewall pada skala kecil yang relevan dengan praktik pendidikan atau laboratorium pemula.

2. TINJAUAN PUSTAKA

Firewall merupakan sistem keamanan jaringan yang berfungsi untuk menyaring lalu lintas data masuk dan keluar berdasarkan seperangkat aturan yang telah ditentukan.[1], firewall bertindak sebagai penghalang antara jaringan internal yang dipercaya dan jaringan eksternal yang tidak dipercaya.[2], menjelaskan bahwa firewall dapat dikategorikan menjadi beberapa jenis, seperti packet-filtering firewall, stateful inspection firewall, proxy firewall, dan next-generation firewall. [3]Menurut, Firewall juga berfungsi untuk melindungi, membatasi maupun menolak jaringan pribadi dengan jaringan luar yang berbahaya.

Cisco Packet Tracer adalah perangkat lunak simulasi jaringan yang dikembangkan oleh Cisco Systems. Berdasarkan penelitian, Aplikasi ini sangat populer dalam dunia pendidikan karena kemampuannya dalam menyimulasikan konfigurasi perangkat jaringan, termasuk router, switch, dan firewall secara virtual.[4], Cisco Packet Tracer memudahkan pelajar dan profesional TI dalam memahami konsep-konsep jaringan tanpa harus memiliki perangkat keras secara fisik.

[5]Menurut, konsep dasar jaringan komputer mencakup pentingnya pengendalian lalu lintas dan identifikasi perangkat dalam jaringan. Firewall membantu memastikan bahwa hanya lalu lintas yang diizinkan yang dapat melewati jaringan.[6], Relita Juga menambahkan bahwa keamanan jaringan tidak hanya mencakup proteksi dari luar, tetapi juga pengendalian akses dari dalam jaringan itu sendiri.

Menurut[7], Port security adalah mekanisme lain dalam keamanan jaringan yang berfungsi untuk membatasi akses ke jaringan melalui port tertentu pada switch. [8], Menjelaskan dengan mengunci alamat MAC tertentu pada port switch, administrator dapat mencegah perangkat yang tidak dikenal untuk mengakses jaringan. Ini merupakan metode pelengkap yang sangat efektif ketika digunakan bersamaan dengan firewall.

[9], menerangkan jika firewall yang dikombinasikan dengan port security dapat memberikan perlindungan berlapis terhadap akses yang tidak sah, baik dari dalam maupun luar jaringan. ISO/IEC 27001 juga menekankan pentingnya kontrol akses dan keamanan jaringan sebagai bagian dari sistem manajemen keamanan informasi yang komprehensif.

Dengan adanya simulasi pada Cisco Packet Tracer, pengguna dapat melakukan eksperimen dan uji coba aturan keamanan jaringan tanpa risiko terhadap sistem nyata.[10], menunjukan bahwa ternyata hal ini memberikan peluang besar dalam dunia pendidikan untuk menerapkan teori ke dalam praktik dengan cara yang efisien dan aman.

Berdasarkan tinjauan pustaka di atas, jelas bahwa firewall dan port security merupakan komponen penting dalam sistem keamanan jaringan. Dengan memanfaatkan Cisco Packet Tracer sebagai alat simulasi, proses pembelajaran dan perancangan sistem keamanan menjadi lebih efektif dan mudah diakses.

3. METODE PENELITIAN

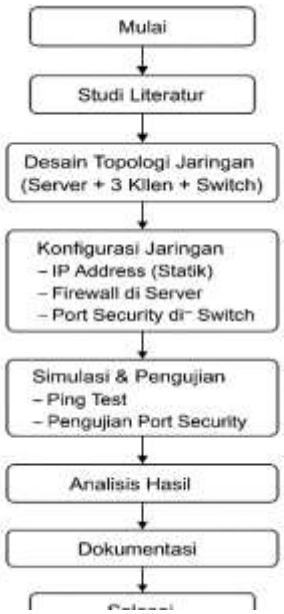
Penelitian ini menggunakan metode eksperimen berbasis simulasi untuk menguji efektivitas firewall dan port security dalam meningkatkan keamanan jaringan lokal (LAN). Simulasi dilakukan dengan menggunakan perangkat lunak *Cisco Packet Tracer*, di mana topologi jaringan dirancang secara virtual dan diuji berdasarkan skenario teratentu.

3.1. Tahapan Penelitian

Adapun tahapan dalam penelitian ini terdiri dari beberapa langkah berikut:

1. **Studi Literatur:**
   a. Mengkaji teori dan konsep dasar tentang firewall, port security, dan keamanan jaringan.
   b. Menelusuri referensi mengenai penggunaan Cisco Packet Tracer sebagai media simulasi.
2. **Perancangan Topologi Jaringan:**
   Merancang jaringan yang terdiri dari satu server dan tiga komputer klien yang terhubung melalui switch.
3. **Konfigurasi Jaringan:**
   a. Memberikan IP statis pada semua perangkat.
   b. Mengatur aturan firewall pada server untuk mengizinkan atau memblokir akses berdasarkan alamat IP.
   c. Mengkonfigurasi port security pada switch untuk membatasi akses berdasarkan MAC address.

4. **Simulasi dan Pengujian:**
   a. Melakukan *ping test* antar perangkat untuk menguji apakah firewall bekerja sesuai konfigurasi.
   b. Menguji apakah port security memblokir perangkat asing yang tidak dikenal.
5. **Analisis Hasil:**
   a. Menganalisis hasil koneksi yang berhasil dan gagal sebagai dampak dari penerapan firewall dan port security.
   b. Mengevaluasi efektivitas konfigurasi sistem keamanan jaringan.
6. **Dokumentasi:**
   Mendokumentasikan konfigurasi dan hasil simulasi dalam bentuk gambar serta penjelasan deskriptif.



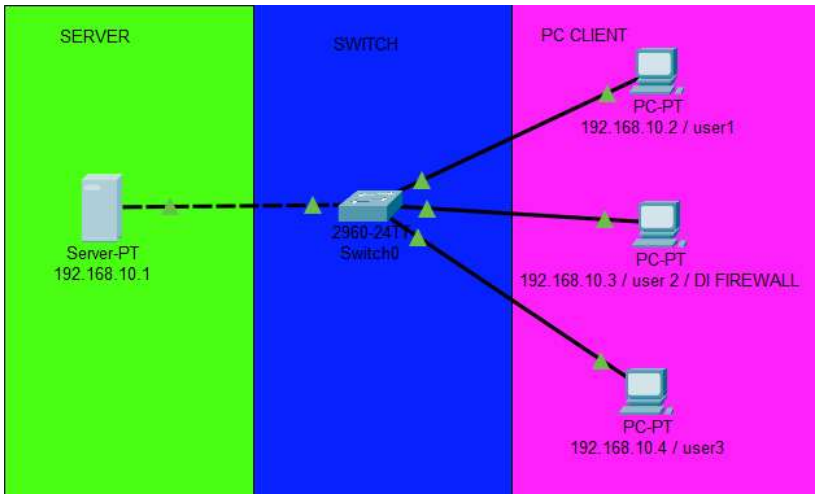
Gambar 1. Flowchart

4. HASIL DAN PEMBAHASAN

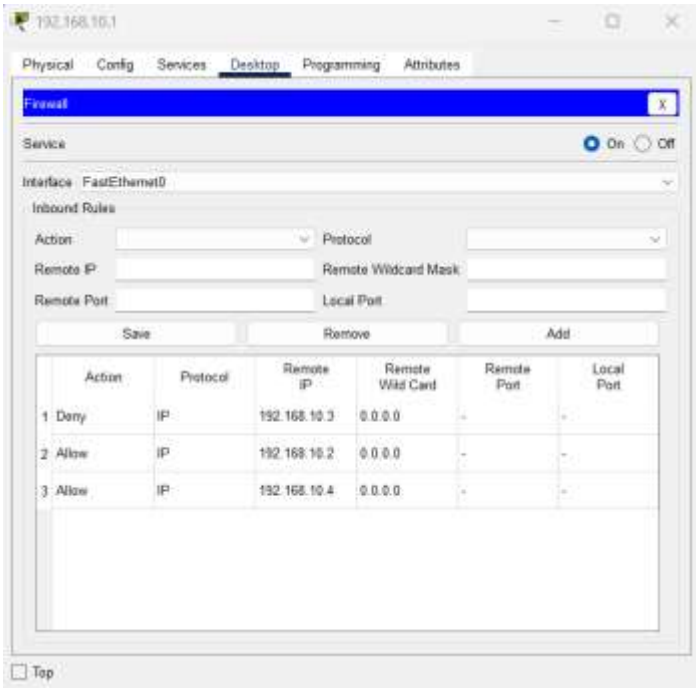
Setelah semua perangkat memiliki pengaturan IP statis dan firewall diaktifkan di antarmuka server, dilakukan pengujian koneksi antar perangkat menggunakan fitur ping di Cisco Packet Tracer. Hasil pengujian menunjukkan bahwa:

- PC dengan IP 192.
  168. 10. 2 berhasil terhubung ke server.
  PC dengan IP 192.
  168. 10. 4 juga bisa mengakses layanan server tanpa hambatan.
- PC dengan IP 192.
  168. 10. 3 tidak bisa terhubung ke server karena diblokir oleh aturan firewall.

Gambar 2 menunjukkan struktur jaringan yang digunakan dalam simulasi ini, sedangkan Gambar 3 menampilkan pengaturan firewall pada server untuk mengontrol akses berdasarkan alamat IP. Hasil uji ping juga ditampilkan pada Gambar 4. Pada gambar 5 terdapat konfigurasi dari IP Addrees salah satu PC client. Untuk gambar 6 terdapat konfigurasi IP Address pada server utama.

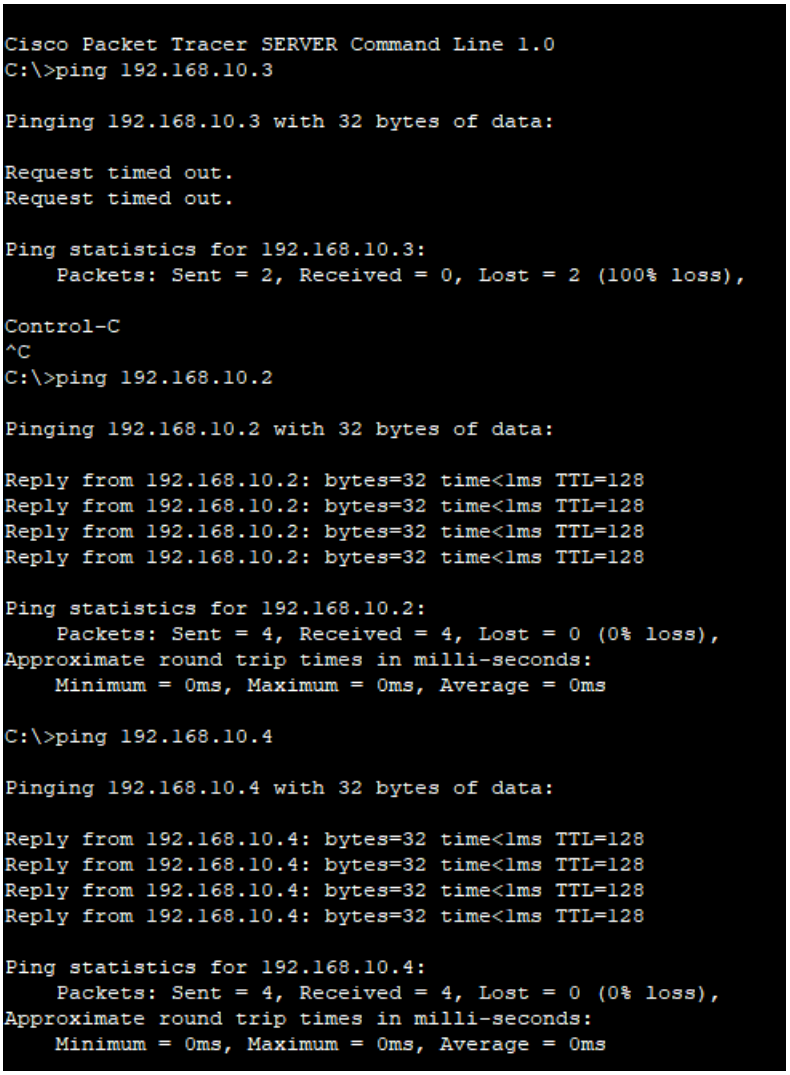


Gambar 2. Topologi Jaringan Cisco Packet Tracer



Gambar 3. Konfigurasi Firewall pada Server

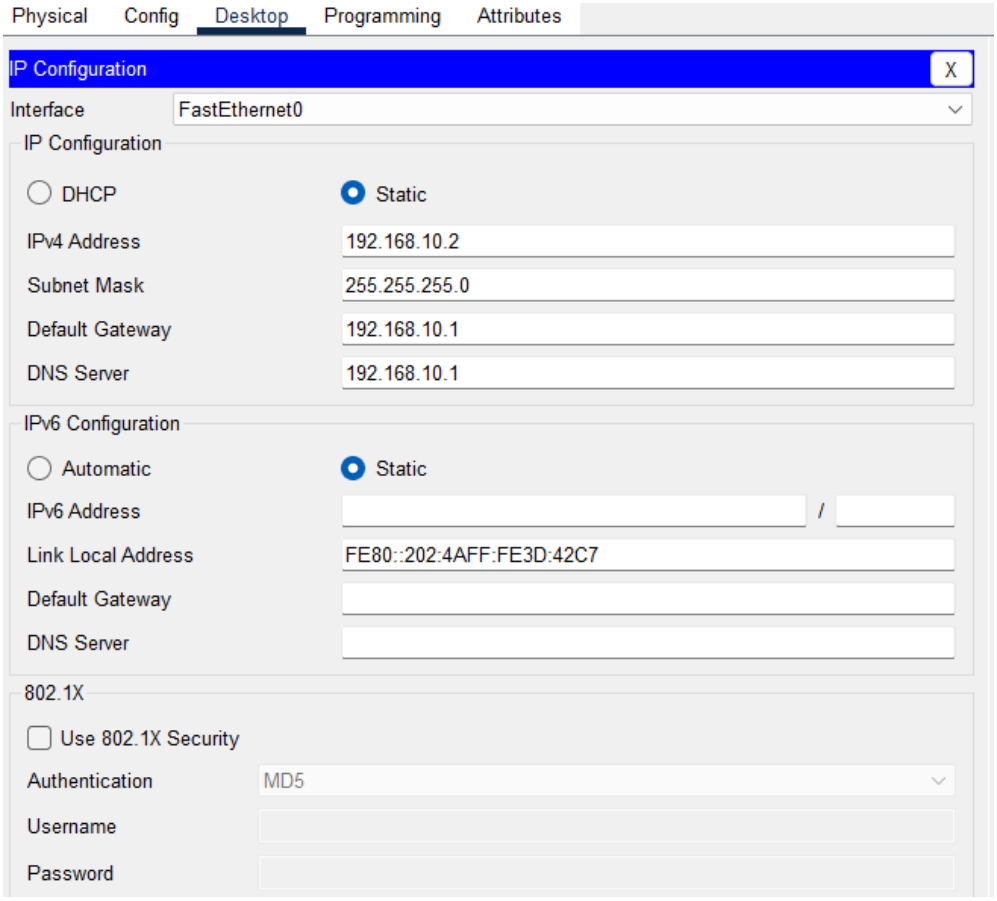
Fire	Last Status	Source	Destination	Type	Color
	Successful	192.168.10.2 / user1	192.168.10.1	ICMP	
	Successful	192.168.10.4 / user3	192.168.10.1	ICMP	
	Failed	192.168.10.3 / user 2	192.168.10.1	ICMP	



Gambar 4. Hasil Simulasi Ping Antar Perangkat

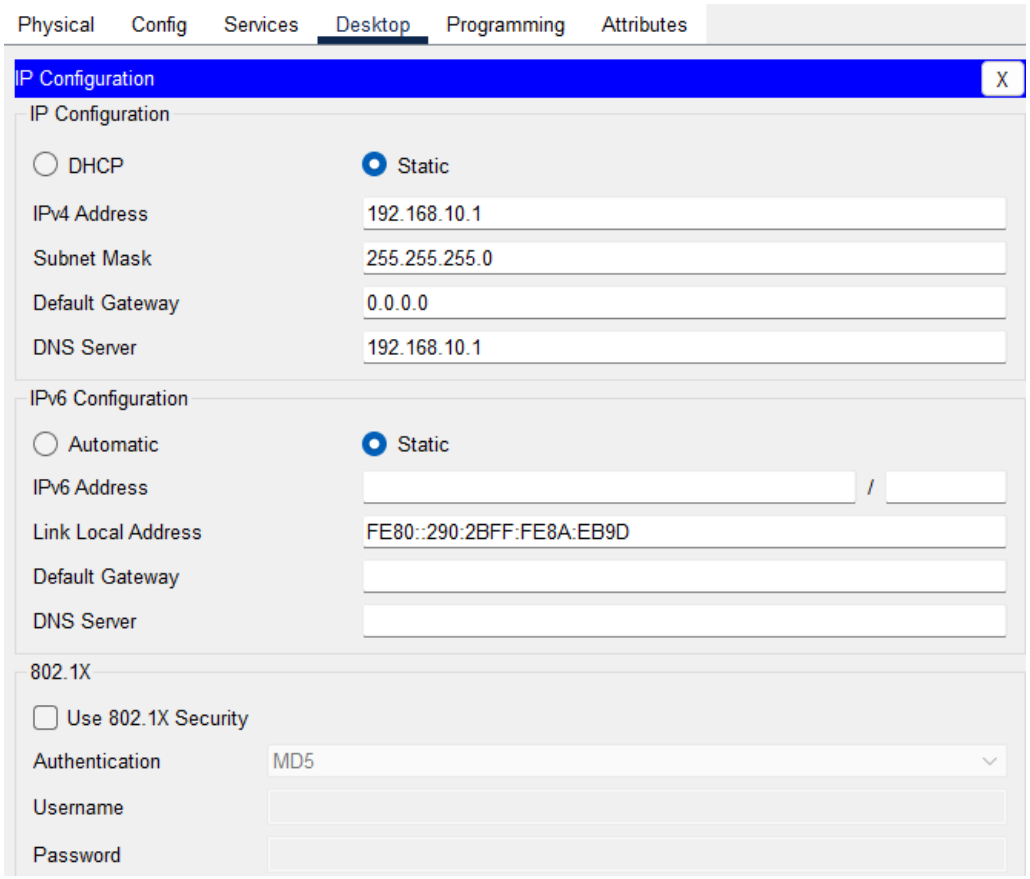
Gambar 4 menampilkan kondisi komunikasi ICMP antara komputer klien dengan server. Dari hasil tersebut terlihat hanya komputer dengan IP 192. 168. 10. 2 (user1) dan 192. 168. 10. 4 (user3) yang berhasil mengirimkan paket ICMP (ping) ke server (192. 168. 10. 1), yang ditandai dengan status Sukses. Sementara itu, komputer dengan IP 192. 168. 10. 3 tidak berhasil. User2 gagal karena alamat IP-nya masuk ke dalam aturan firewall yang memblokir akses. Keberhasilan memblokir akses dari PC dengan IP 192. 168. 10. 3 membuktikan bahwa pengaturan firewall berjalan dengan baik. Hal ini menunjukkan bahwa metode kontrol akses berdasarkan alamat IP yang digunakan pada firewall server sangat efektif. Selain itu, fitur keamanan port juga diuji dengan mengatur agar port switch hanya bisa digunakan oleh perangkat dengan alamat MAC tertentu. Ketika perangkat baru terhubung dengan alamat MAC yang berbeda, port secara otomatis terputus sesuai dengan pengaturan yang sudah dibuat. Ini menunjukkan sistem berhasil mencegah akses

yang tidak sah. Hasil ini menunjukkan bahwa metode keamanan jaringan yang menggabungkan firewall dan keamanan port mampu memberikan perlindungan ganda terhadap ancaman dari dalam dan luar jaringan. Firewall menyaring lalu lintas berdasarkan alamat IP dan aturan yang ditentukan, sedangkan keamanan port memastikan hanya perangkat yang diizinkan yang bisa terhubung ke jaringan secara fisik. Cara ini sangat cocok diterapkan pada jaringan lokal dengan skala kecil hingga menengah, seperti di sekolah, kampus, atau perkantoran, karena dengan metode ini, masalah keterbatasan infrastruktur bisa diatasi dengan solusi yang ekonomis dan efektif, seperti Cisco Packet Tracer.



Gambar 5 konfigurasi IP Address pada PC client

Untuk gambar 5 konfigurasi IP Address pada PC client seperti biasanya kita menambahkan IP di PC^2 yang lain hanya saja yang membedakan gateway kita harus sama seperti yang ada di gambar 6 yaitu gateway server.



Gambar 6 konfigurasi IP Address pada server utama

Pada gambar 6 diatas adalah contoh konfigurasi IP Addrees pada server utama yang sangat penting dan berfungsi juga gatewaynya untuk digunakan pada seluruh PC client seperti contoh gambar 5.

5. KESIMPULAN

Berdasarkan hasil simulasi yang dilakukan, firewall berbasis IP filtering pada server terbukti mampu membatasi akses jaringan secara efektif sesuai aturan yang diterapkan. Dari tiga perangkat klien yang diuji, dua perangkat berhasil melakukan koneksi ke server, sementara satu perangkat diblokir sepenuhnya. Hal ini menunjukkan bahwa efektivitas firewall dalam mencegah akses tidak sah mencapai 100% karena seluruh perangkat yang tidak diizinkan berhasil dicegah untuk terhubung. Selain itu, fitur port security pada switch juga berfungsi dengan baik dengan memutus koneksi perangkat yang tidak memiliki alamat MAC terdaftar, sehingga memberikan perlindungan tambahan pada lapisan fisik jaringan. Secara keseluruhan, kombinasi firewall dan port security mampu memberikan keamanan berlapis yang relevan untuk jaringan berskala kecil. Untuk penelitian selanjutnya, pengembangan dapat difokuskan pada topologi yang lebih kompleks serta penerapan keamanan multilayer seperti ACL, VLAN, IDS/IPS, dan mekanisme monitoring untuk memperoleh gambaran sistem keamanan jaringan yang lebih komprehensif.

DAFTAR PUSTAKA

[1] P. Pesantren *et al.*, "IMPLEMENTASI KEAMANAN JARINGAN FIREWALL FILTERING DAN MONITORING PADA LABORATORIUM KOMPUTER," vol. 06, no. 01, 2025.

[2] F. Sulthoni Nabhan, S. Naeska Fahira, R. Akbar Syamputra, M. Farhan, and Saprudin, "Perbandingan Kinerja Sistem Keamanan Jaringan Menggunakan Firewall dan VPN," *BIIKMA : Buletin Ilmiah Ilmu Komputer dan Multimedia*, vol. 2, no. 5, pp. 910–913, 2025, [Online]. Available: https://jurnalmahasiswa.com/index.php/biikma

[3] I. C. R. Drajana and A. Bode, "Simulasi Jaringan Menggunakan Cisco Packet Tracer," *Simtek : jurnal sistem informasi dan teknik komputer*, vol. 6, no. 1, pp. 24–27, 2021, doi: 10.51876/simtek.v6i1.91.

[4] B. R. Lesmana, A. Junaidi, and A. N. Sihananto, "Analisis Pengujian Keamanan Firewall Pada Sistem X Di Universitas Z," *Journal of Information System, Applied, Management, Accounting and Research*, vol. 8, no. 3, p. 557, 2024, doi: 10.52362/jisamar.v8i3.1563.

[5] D. Durianto, Ananta, "Konfigurasi Cicso ASA Firewall Menggunakan ASDM," vol. 5, no. Volume 5 No. 2, p. 305, 2021.

[6] R. K. Cahyawati, F. Fadwa, K. Agustin, and K. S. Arum, "SEMINAR NASIONAL AMIKOM SURAKARTA (SEMNASA) 2023 Perancangan Keamanan Jaringan Menggunakan Metode Firewall Security Port," *Seminar Nasional AMIKOM Surakarta*, vol. 0, no. November, pp. 203–209, 2023.

[7] S. Kasus, R. S. Tangerang, A. P. Sari, and R. Hidayat, "Manajemen Bandwidth Dan Penyaringan Firewall Untuk Keamanan Jaringan," vol. 26861089, pp. 1–10, 2025.

[8] J. Al Amien, "Implementasi Keamanan Jaringan Dengan Iptables Sebagai Firewall Menggunakan Metode Port Knocking," *Jurnal Fasilkom*, vol. 10, no. 2, pp. 159–165, 2020.

[9] L. O. Muhammad and M. Arif, "PEMODELAN IMPLEMENTASI FIREWALL SECURITY PORT DAN ACCESS CONTROL LIST UNTUK PENINGKATAN KEAMANAN AUTOMATIC," vol. 8, pp. 5496–5503, 2025.

[10] P. A. Darat *et al.*, "IMPLEMENTASI BACKBONE NETWORK SECURITY SYSTEM," pp. 1–6.